REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is obvious under the provisions of 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are in allowable form.

I. REJECTION OF CLAIMS 1-5 AND 10-12 UNDER 35 U.S.C. §103

Claims 1-5 and 10-12 stand rejected as being unpatentable over the Purtell et al. patent (U.S. 6,950,947, issued September 27, 2005, hereinafter "Purtell"). The Applicants note that Page 2 of the Final Office Action states that the claims are rejected over Purtell in view of the Fox et al. patent (U.S. 7,096,502, issued August 22, 2006, hereinafter "Fox"). However, the Final Office Action does not explain specifically how Fox has been applied to the claims, and, in fact, Fox is not mentioned again anywhere in the Office Action. As such, the Examiner instructed the Applicants in a voice message dated October 14, 2009 to treat the rejection as a rejection over Purtell only. As such, the Applicants' arguments do not address Fox, and the Applicants respectfully traverse the rejection over Purtell.

Particularly, the Examiner's attention is directed to the fact that Purtell fails to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the belief states indicate probabilistic beliefs of the sensors regarding states of system resources or services, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12.

By contrast, Purtell discloses a set of peer firewalls that share direct measurements of transmission control protocol (TCP) control state. Specifically, the firewalls exchange common TCP control blocks (CCBs) that contain objective information about the physical connection between two entities connected via TCP (such as "round trip time (RTT) and variance, the congestion-controlled window, local and remote MSS [maximum segment size], and retransmission and error rate," Purtell, column 4, lines 15-19). Thus, the shared data is not probabilistic, as claimed by the Applicants, but rather has definite, directly measurable values.

The Examiner appeared to acknowledge Purtell's failure to teach the use and adjustment of probabilistic belief states in the Office Action dated February 26, 2009.

Specifically, in response to the Applicants' previous arguments regarding this shortcoming in the teachings of Purtell, the Examiner withdrew a 35 U.S.C. §102 rejection over Purtell, and instead applied a new ground of rejection (which did not use Purtell) to the claims (*See, e.g.*, Page 2 of the February 26, 2009 Office Action).

Thus, Purtell fails to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the belief states indicate probabilistic beliefs of the sensors regarding states of system resources or services, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12. Specifically, Applicants' claims 1, 4, 5, and 10 - 12 positively recite:

1. A method for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor information about a belief state of the second sensor, said belief state of the second sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to a suspicious activity in the intrusion detection system is improved. (Emphasis added)

4. A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a probabilistic belief of the second sensor regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the first sensor, so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system. (Emphasis added)

5. A method for enhancing a sensitivity of an intrusion detection system that

monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system. (Emphasis added)

10. A sensor device containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor information about a belief state of the second sensor, said belief state of the second sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a current state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to a suspicious activity in the intrusion detection system is improved. (Emphasis added)

11. A sensor device containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a probabilistic belief of the second sensor regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding an apparent normal, degraded or compromised current state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system. (Emphasis added)

12. A sensor device containing an executable program for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each

maintaining belief regarding a service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a current existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system. (Emphasis added)

As discussed above, Purtell fails to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the belief states indicate probabilistic beliefs of the sensors regarding states of system resources or services, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12. Therefore, the Applicants submit that independent claims 1, 4, 5, and 10 - 12 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 2-3 depend from claim 1 and recite at least the same patentable features recited in claim 1. As such, and for at least the same reasons set forth above, the Applicants submit that claims 2-3 are also not obvious over the teachings of Purtell. Therefore, the Applicants submit that dependent claims 2-3 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

II. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Kin-Wah Tong, Esq. at (732) 842-8110 x130 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

October 19, 2009
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 842-8110 x130

Wall & Tong, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702